0020HQ" 96/11/50

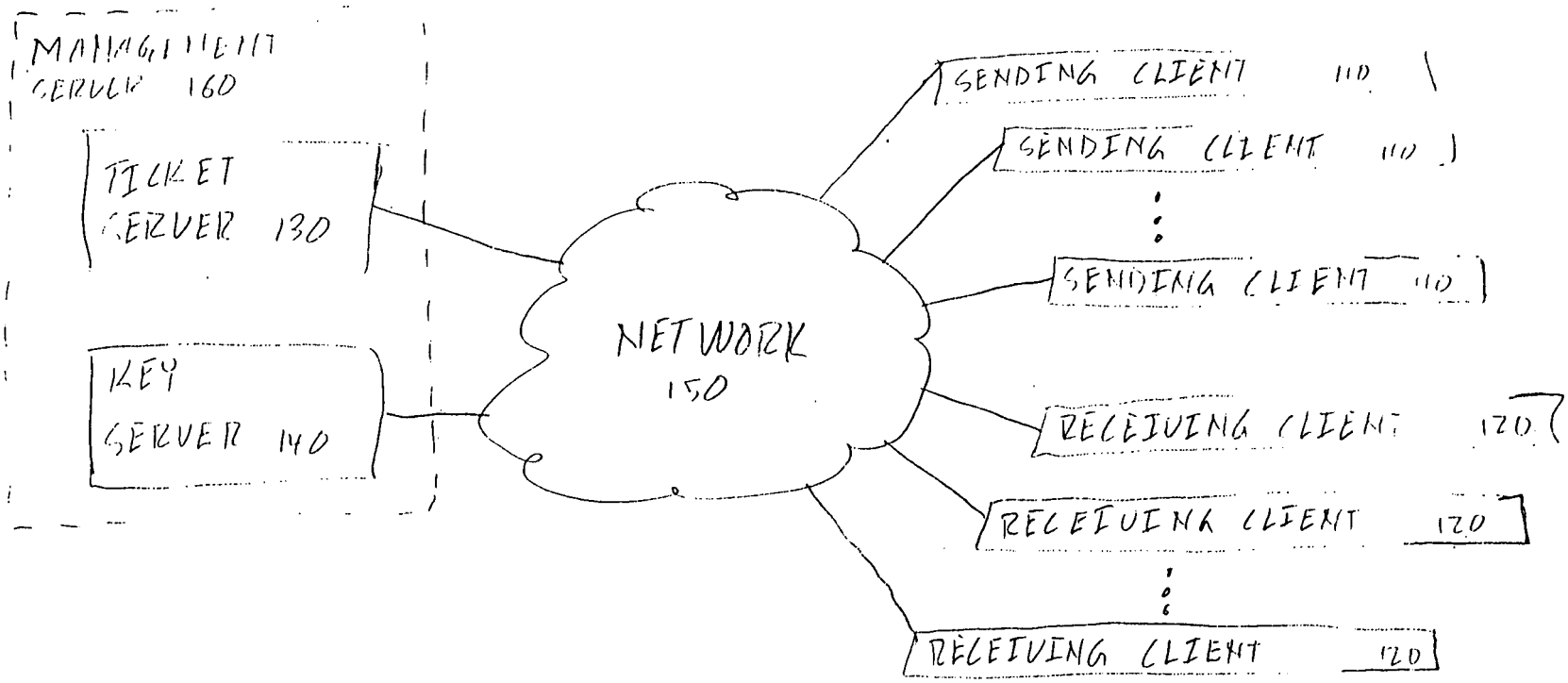


FIG. 1

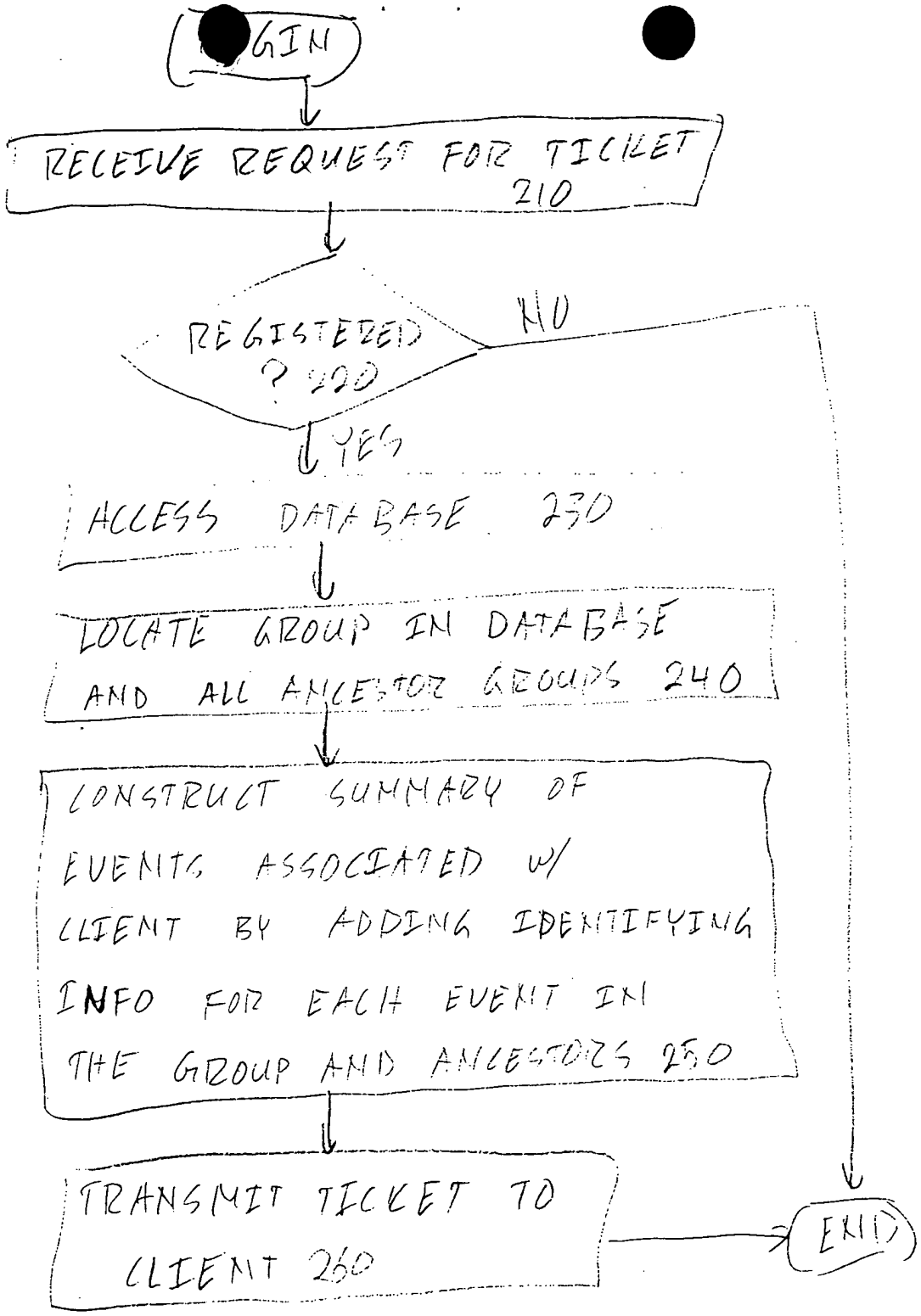

BEGIN
RECEIVE REQUEST FOR TICKET 210
REGISTERED ? 220
NO
YES
ACCESS DATABASE 230
LOCATE GROUP IN DATABASE AND ALL ANCESTOR GROUPS 240
CONSTRUCT SUMMARY OF EVENTS ASSOCIATED W/ CLIENT BY ADDING IDENTIFYING INFO FOR EACH EVENT IN THE GROUP AND ANCESTORS 250
TRANSMIT TICKET TO CLIENT 260
END

FIG. 2.

ASSOCIATIVE DATABASE

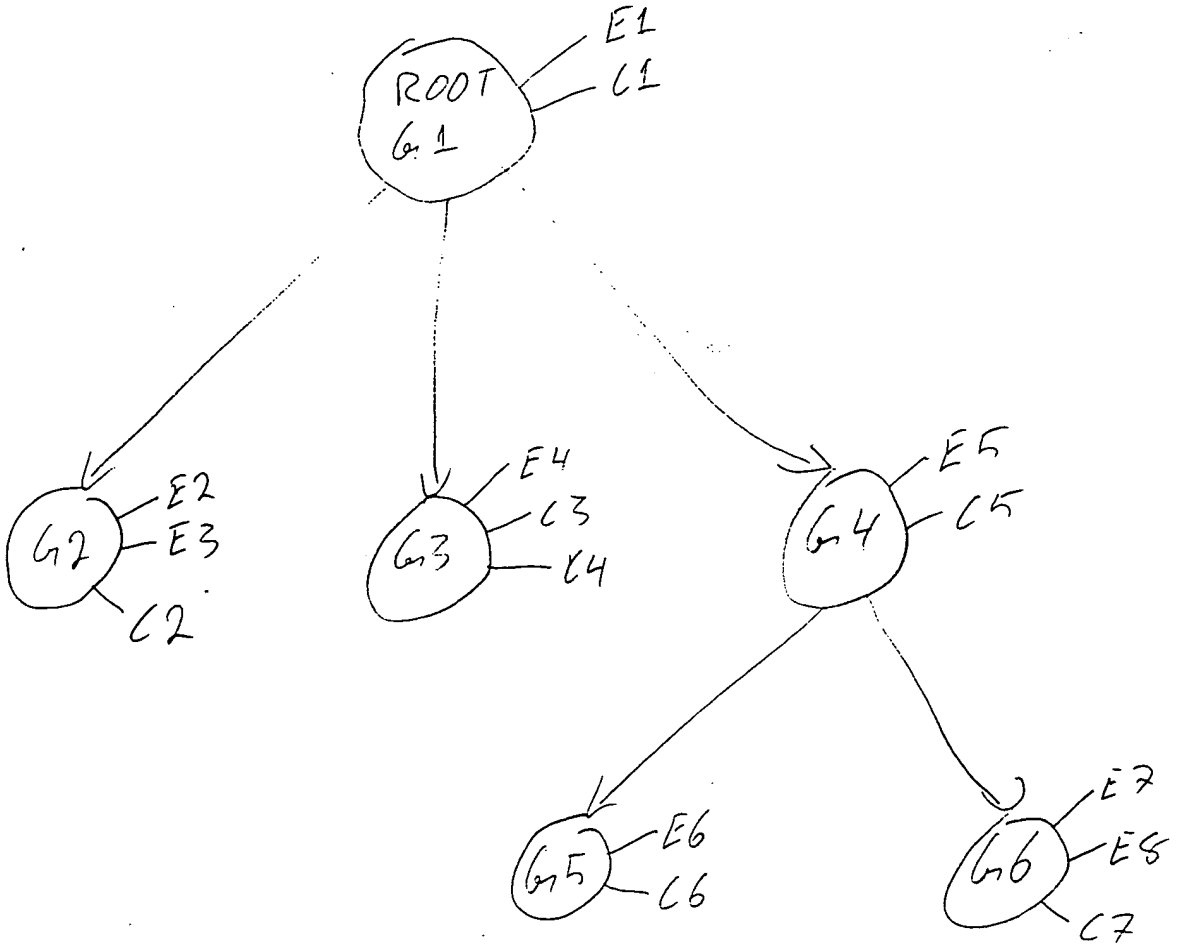


FIG. 3

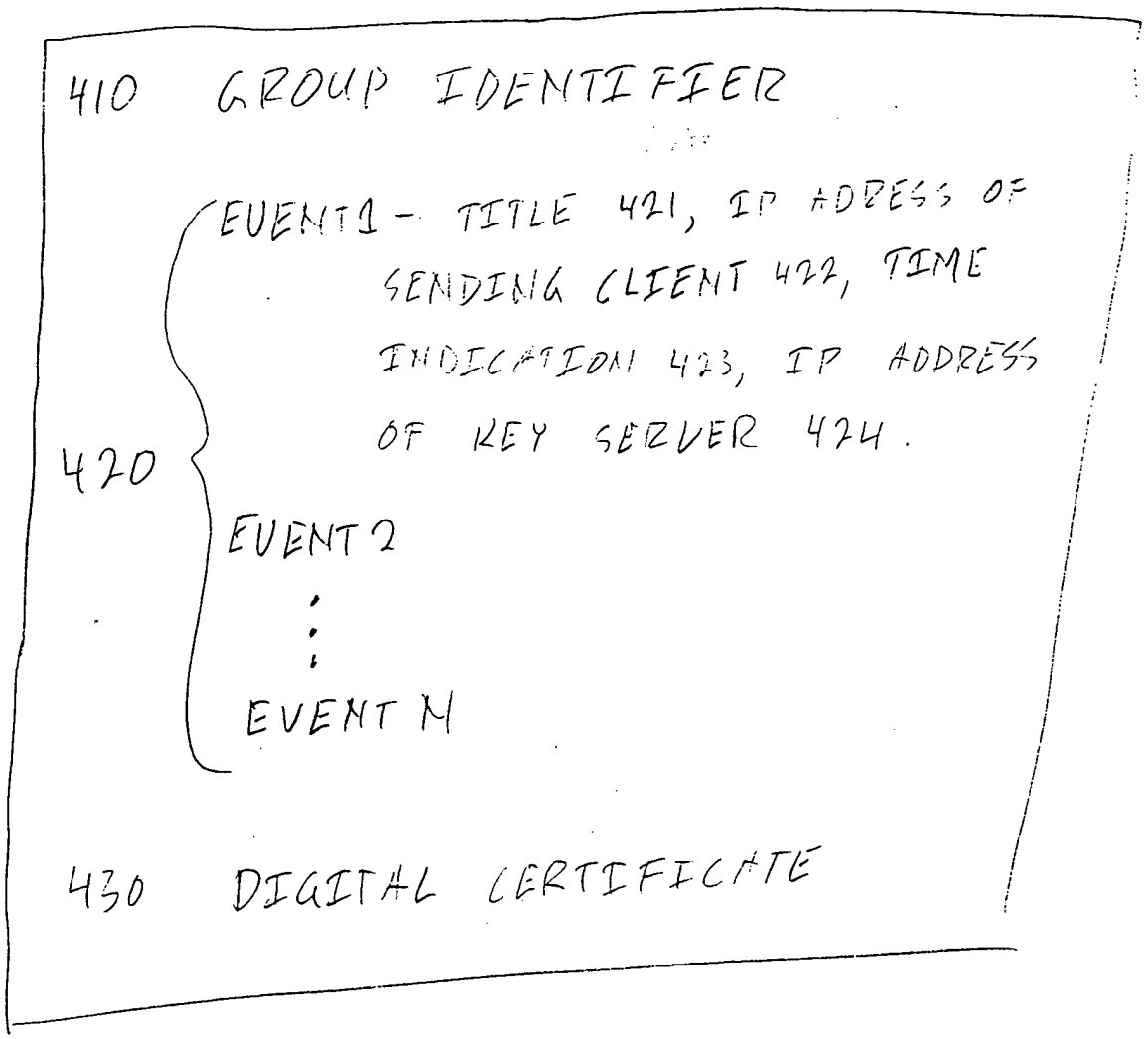

410 GROUP IDENTIFIER
420
EVENT 1 - TITLE 421, IP ADDRESS OF SENDING CLIENT 422, TIME INDICATION 423, IP ADDRESS OF KEY SERVER 424.
EVENT 2
EVENT M
430 DIGITAL CERTIFICATE

FIG. 4

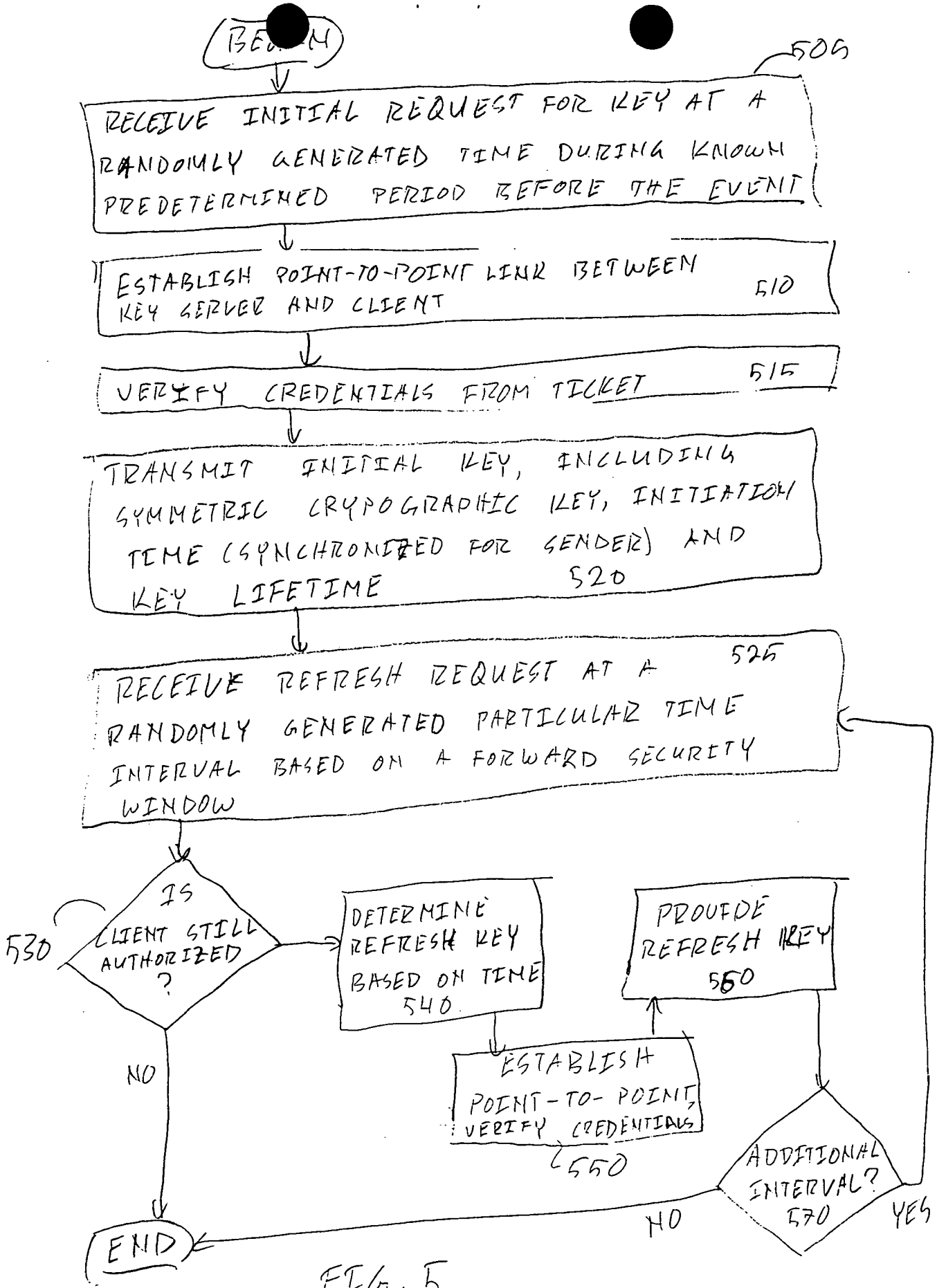
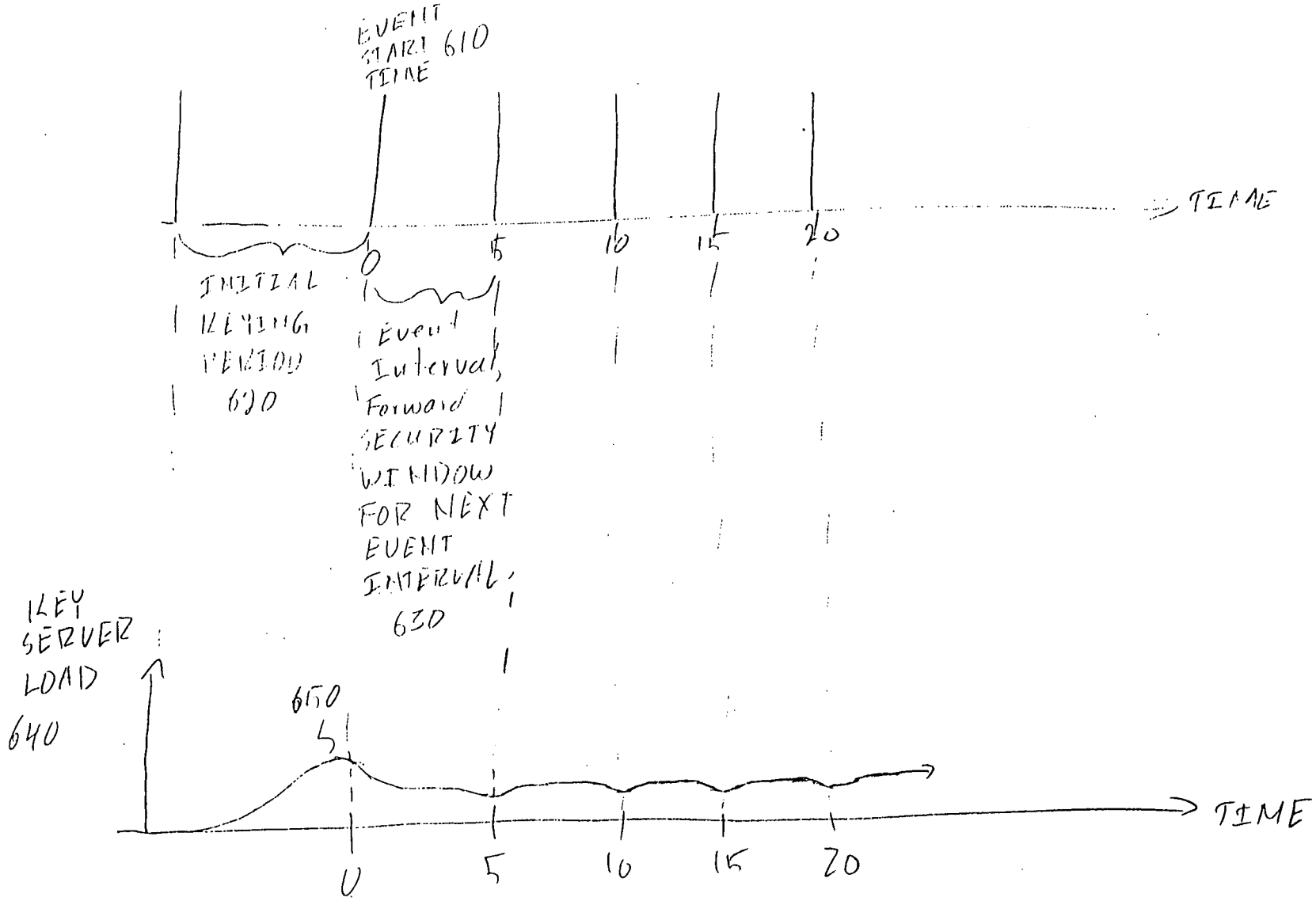

BEGIN
505
RECEIVE INITIAL REQUEST FOR KEY AT A RANDOMLY GENERATED TIME DURING KNOWN PREDETERMINED PERIOD BEFORE THE EVENT
ESTABLISH POINT-TO-POINT LINK BETWEEN KEY SERVER AND CLIENT
510
VERIFY CREDENTIALS FROM TICKET
515
TRANSMIT INITIAL KEY, INCLUDING SYMMETRIC CRYPOGRAPHIC KEY, INITIATION TIME (SYNCHRONIZED FOR SENDER) AND KEY LIFETIME
520
RECEIVE REFRESH REQUEST AT A RANDOMLY GENERATED PARTICULAR TIME INTERVAL BASED ON A FORWARD SECURITY WINDOW
525
IS CLIENT STILL AUTHORIZED ?
530
NO
DETERMINE REFRESH KEY BASED ON TIME
540
ESTABLISH POINT-TO-POINT, VERIFY CREDENTIALS
550
PROVIDE REFRESH KEY
560
ADDITIONAL INTERVAL?
570
YES
NO
END

FIG. 5

FIG. 6


EVENT START TIME 610
TIME
0
5
10
15
20
INITIAL KEYING PERIOD 620
EVENT Interval, Forward SECURITY WINDOW FOR NEXT EVENT INTERVAL 630
KEY SERVER LOAD
640
650
TIME
0
5
10
15
20

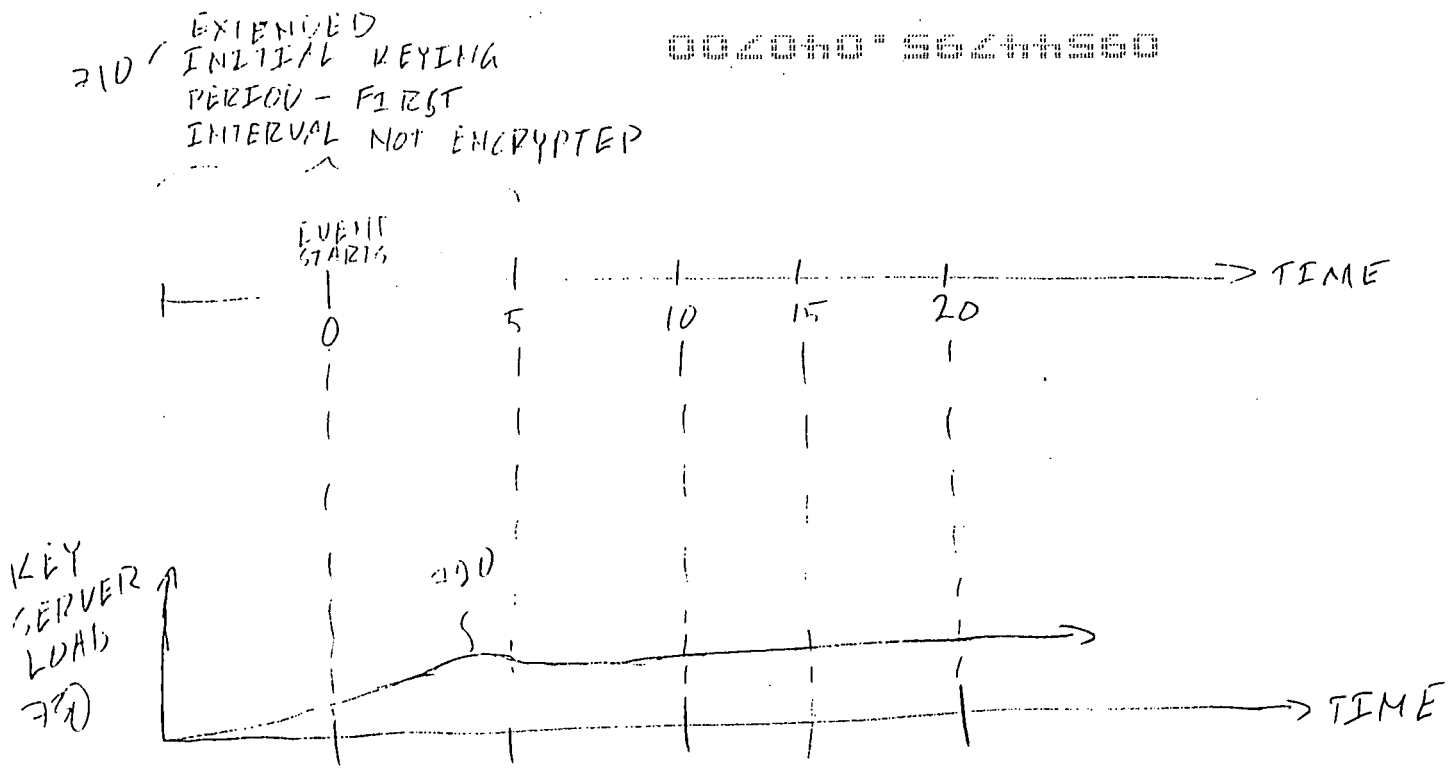

210
EXTENDED INITIAL KEYING PERIOD - FIRST INTERVAL NOT ENCRYPTED
EVENT STARTS
0
5
10
15
20
TIME
KEY SERVER LOAD
220
TIME

FIG. 7

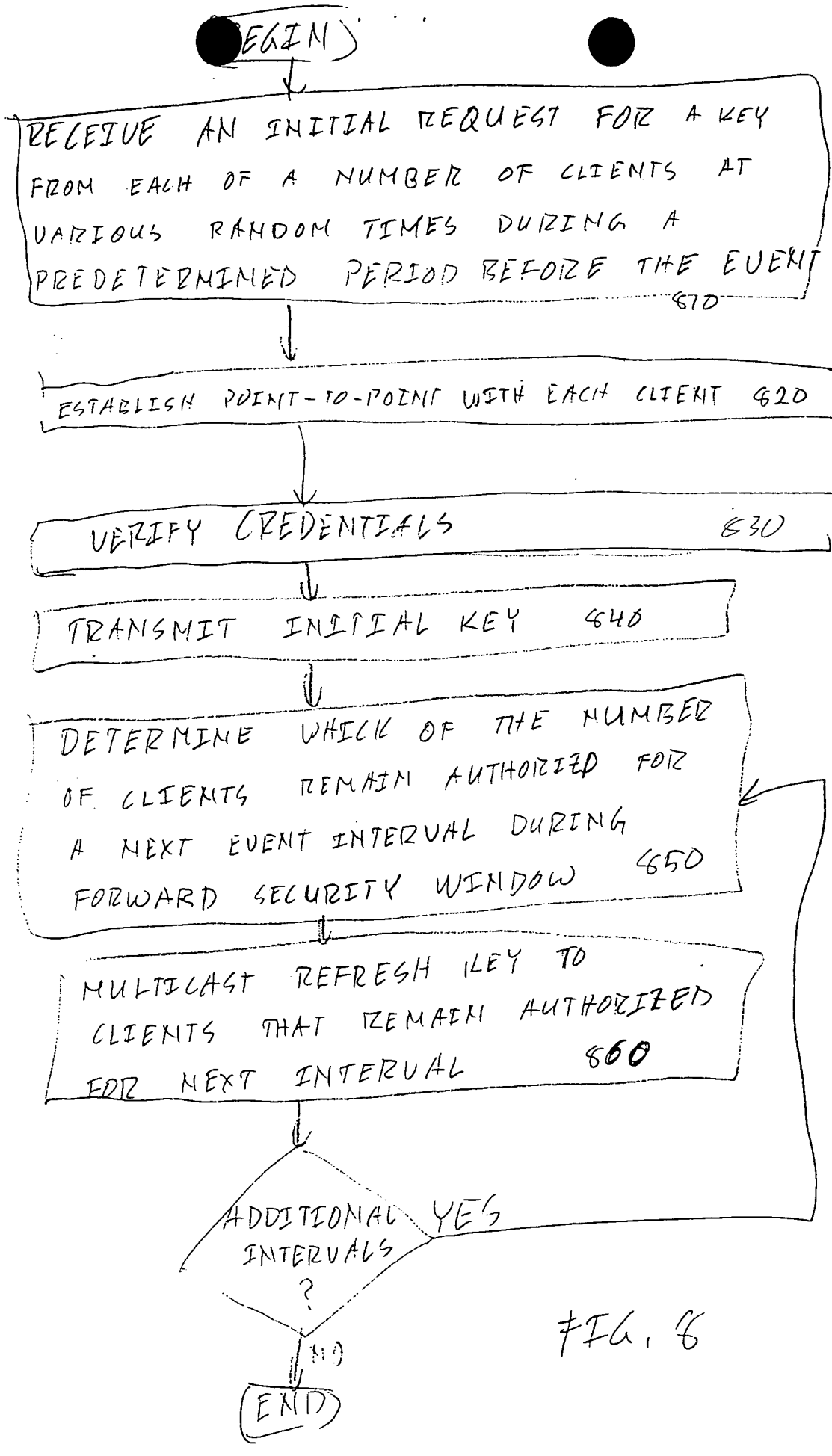

BEGIN
RECEIVE AN INITIAL REQUEST FOR A KEY FROM EACH OF A NUMBER OF CLIENTS AT VARIOUS RANDOM TIMES DURING A PREDETERMINED PERIOD BEFORE THE EVENT
610
ESTABLISH POINT-TO-POINT WITH EACH CLIENT 620
VERIFY CREDENTIALS 630
TRANSMIT INITIAL KEY 640
DETERMINE WHICH OF THE NUMBER OF CLIENTS REMAIN AUTHORIZED FOR A NEXT EVENT INTERVAL DURING FORWARD SECURITY WINDOW 650
MULTICAST REFRESH KEY TO CLIENTS THAT REMAIN AUTHORIZED FOR NEXT INTERVAL 660
ADDITIONAL INTERVALS ?
YES
NO
END

FIG. 6

FIG. 9

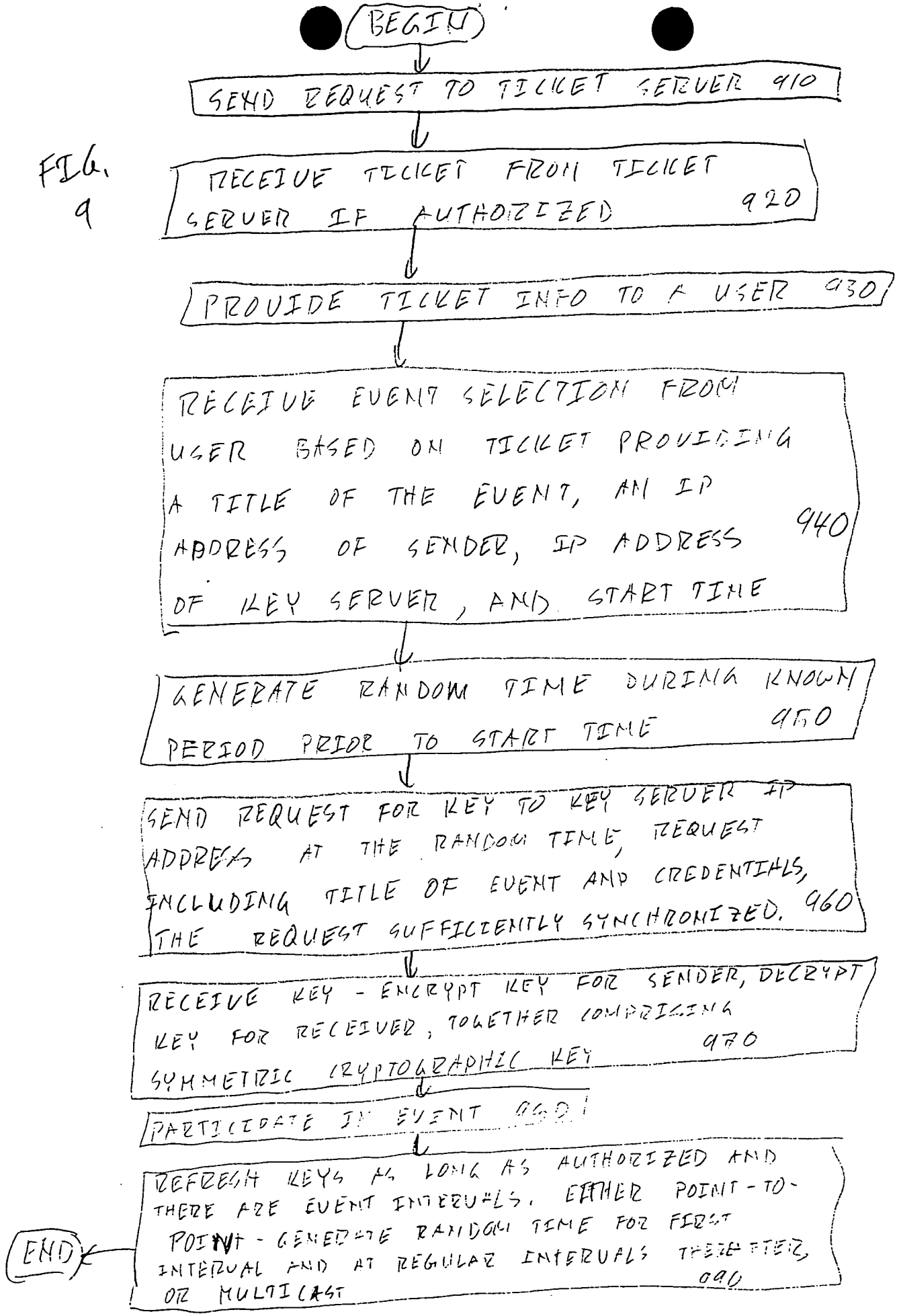
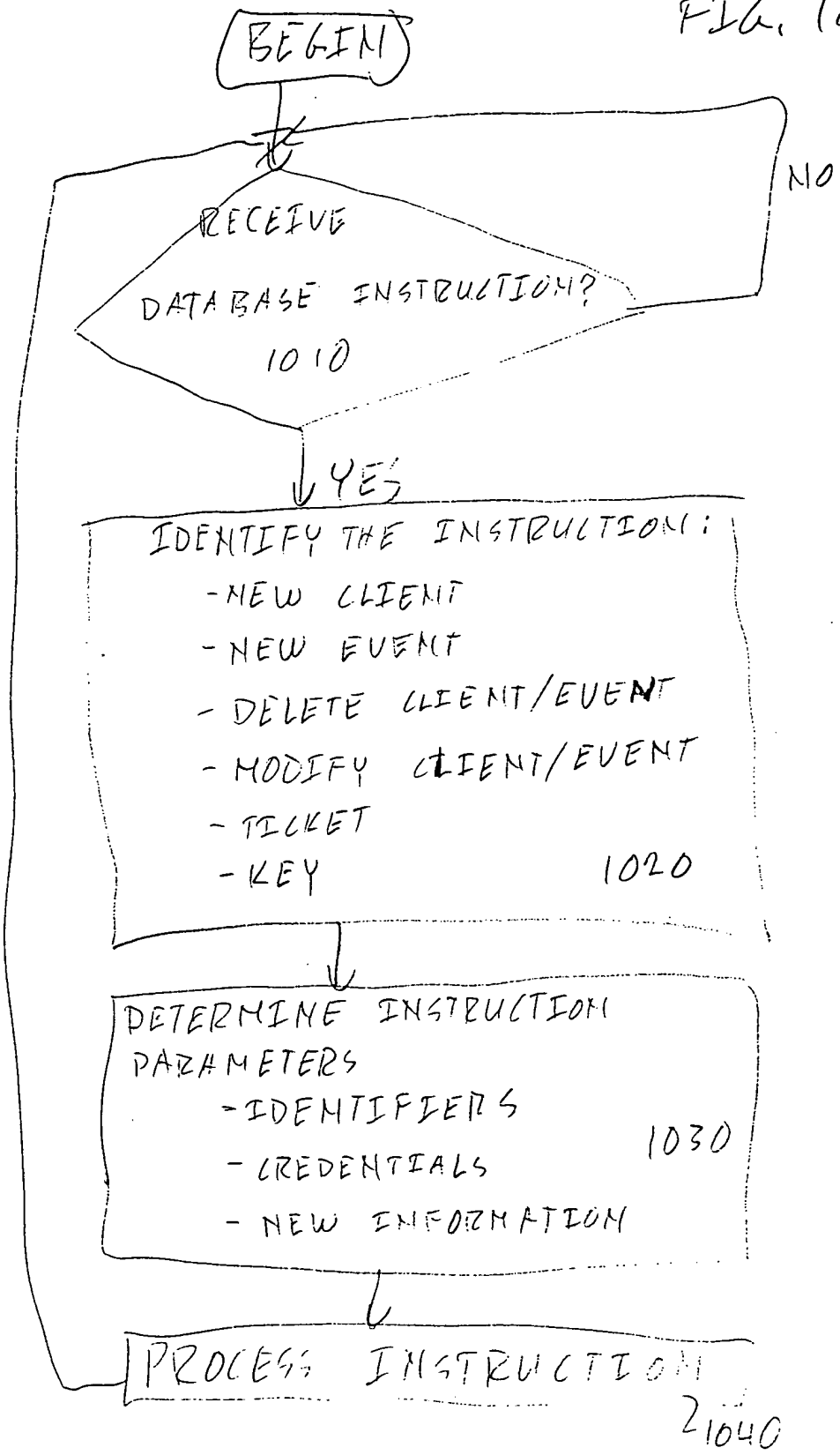

BEGIN
SEND REQUEST TO TICKET SERVER 910
RECEIVE TICKET FROM TICKET SERVER IF AUTHORIZED 920
PROVIDE TICKET INFO TO A USER 930
RECEIVE EVENT SELECTION FROM USER BASED ON TICKET PROVIDING A TITLE OF THE EVENT, AN IP ADDRESS OF SENDER, IP ADDRESS OF KEY SERVER, AND START TIME 940
GENERATE RANDOM TIME DURING KNOWN PERIOD PRIOR TO START TIME 950
SEND REQUEST FOR KEY TO KEY SERVER IP ADDRESS AT THE RANDOM TIME, REQUEST INCLUDING TITLE OF EVENT AND CREDENTIALS, THE REQUEST SUFFICIENTLY SYNCHRONIZED. 960
RECEIVE KEY - ENCRYPT KEY FOR SENDER, DECRYPT KEY FOR RECEIVED, TOGETHER COMPRISING SYMMETRIC CRYPTOGRAPHIC KEY 970
PARTICIPATE IN EVENT 980
REFRESH KEYS AS LONG AS AUTHORIZED AND THERE ARE EVENT INTERVALS. EITHER POINT-TO-POINT - GENERATE RANDOM TIME FOR FIRST INTERVAL AND AT REGULAR INTERVALS THEREAFTER, OR MULTICAST 990
END

FIG. 10


BEGIN
RECEIVE DATABASE INSTRUCTION?
1010
NO
YES
IDENTIFY THE INSTRUCTION:
- NEW CLIENT
- NEW EVENT
- DELETE CLIENT/EVENT
- MODIFY CLIENT/EVENT
- TICKET
- KEY
1020
DETERMINE INSTRUCTION PARAMETERS
- IDENTIFIERS
- CREDENTIALS
- NEW INFORMATION
1030
PROCESS INSTRUCTION
1040

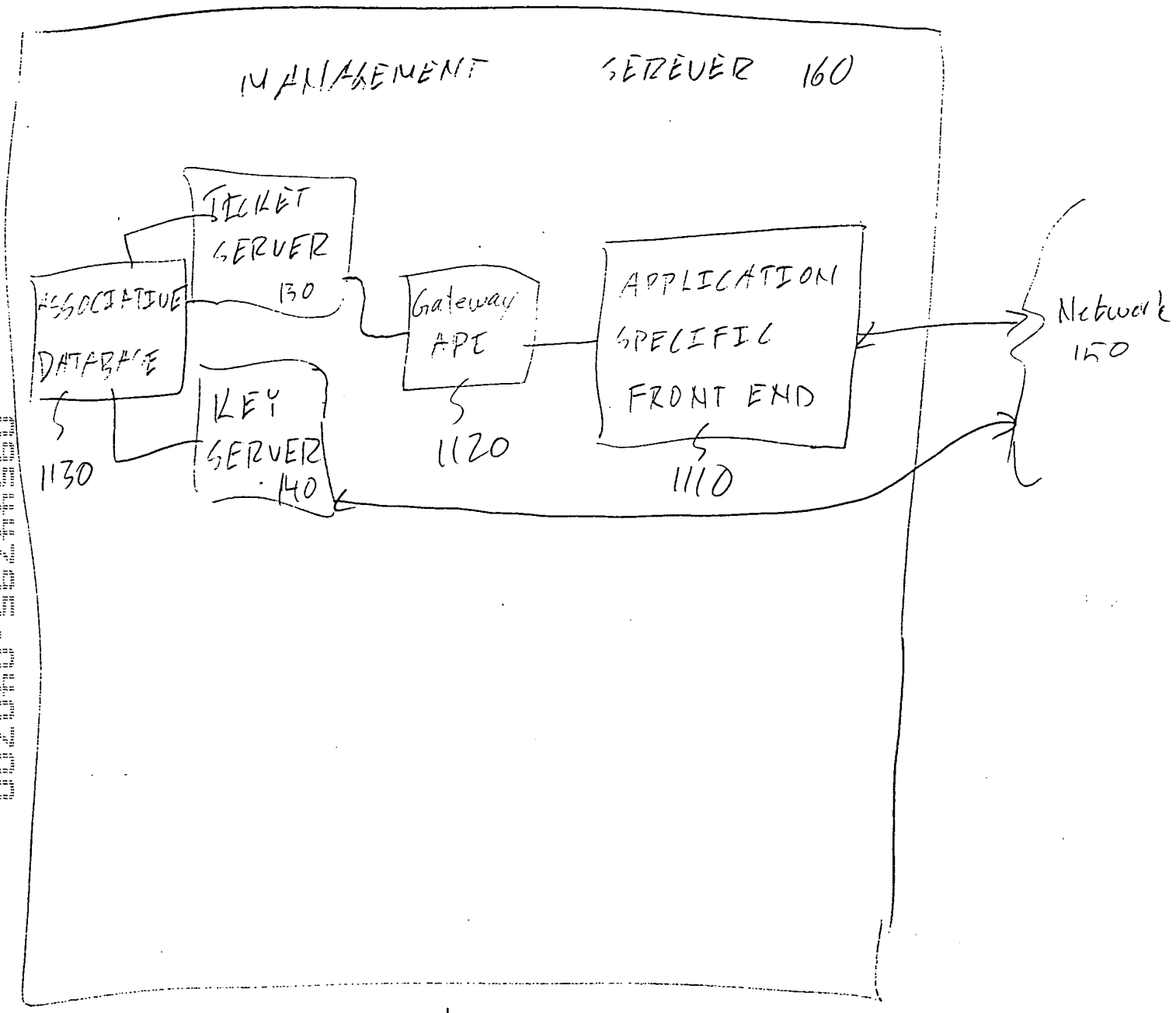
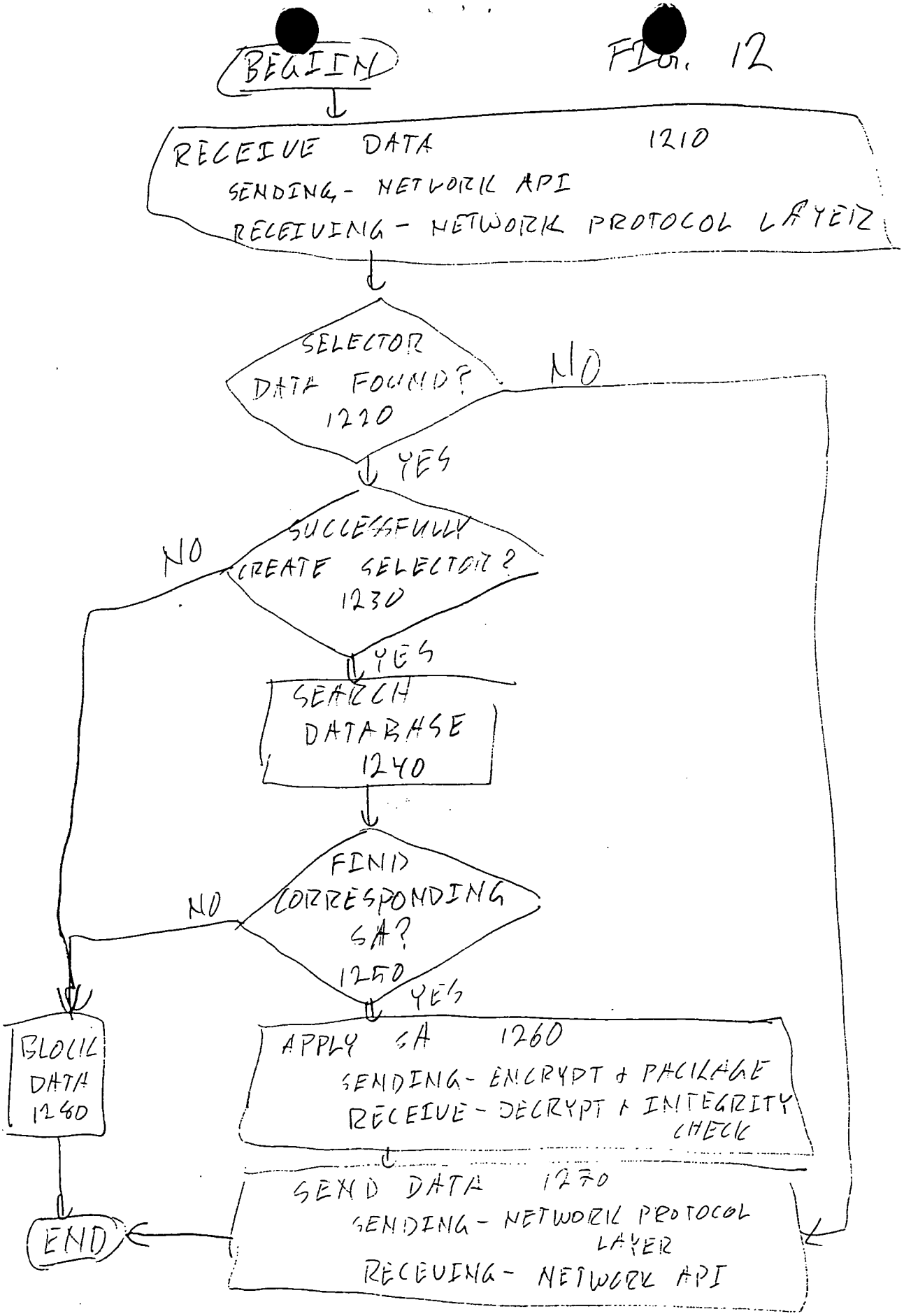

MANAGEMENT SERVER 160
TICKET SERVER 130
ASSOCIATIVE DATABASE
1130
KEY SERVER 140
Gateway API
1120
APPLICATION SPECIFIC FRONT END
1110
Network 150

FIG. 11

FIG. 12


BEGIN
RECEIVE DATA 1210
SENDING - NETWORK API
RECEIVING - NETWORK PROTOCOL LAYER
SELECTOR DATA FOUND? 1220
NO
YES
SUCCESSFULLY CREATE SELECTOR? 1230
NO
YES
SEARCH DATABASE 1240
FIND CORRESPONDING SA? 1250
NO
YES
BLOCK DATA 1260
APPLY SA 1260
SENDING - ENCRYPT & PACKAGE
RECEIVE - DECRYPT & INTEGRITY CHECK
SEND DATA 1270
SENDING - NETWORK PROTOCOL LAYER
RECEIVING - NETWORK API
END

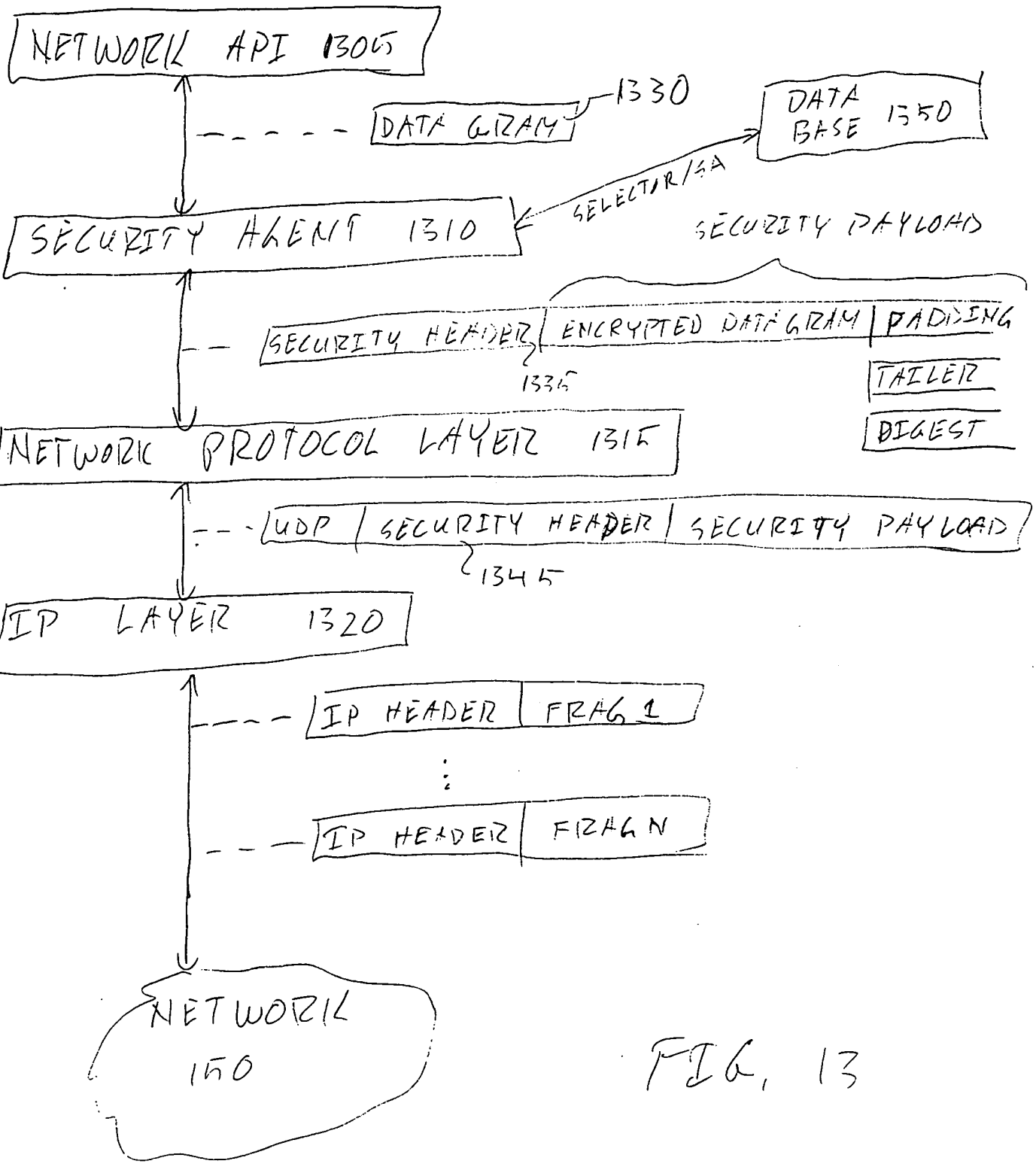

NETWORK API 1305
DATA GRAM
1330
DATA BASE 1350
SELECTOR/SA
SECURITY AGENT 1310
SECURITY PAYLOAD
SECURITY HEADER
ENCRYPTED DATAGRAM
PADDING
TAILER
DIGEST
1335
NETWORK PROTOCOL LAYER 1315
UDP
SECURITY HEADER
SECURITY PAYLOAD
1345
IP LAYER 1320
IP HEADER
FRAG 1
IP HEADER
FRAG N
NETWORK 150

FIG. 13

08208A0 "5624h560

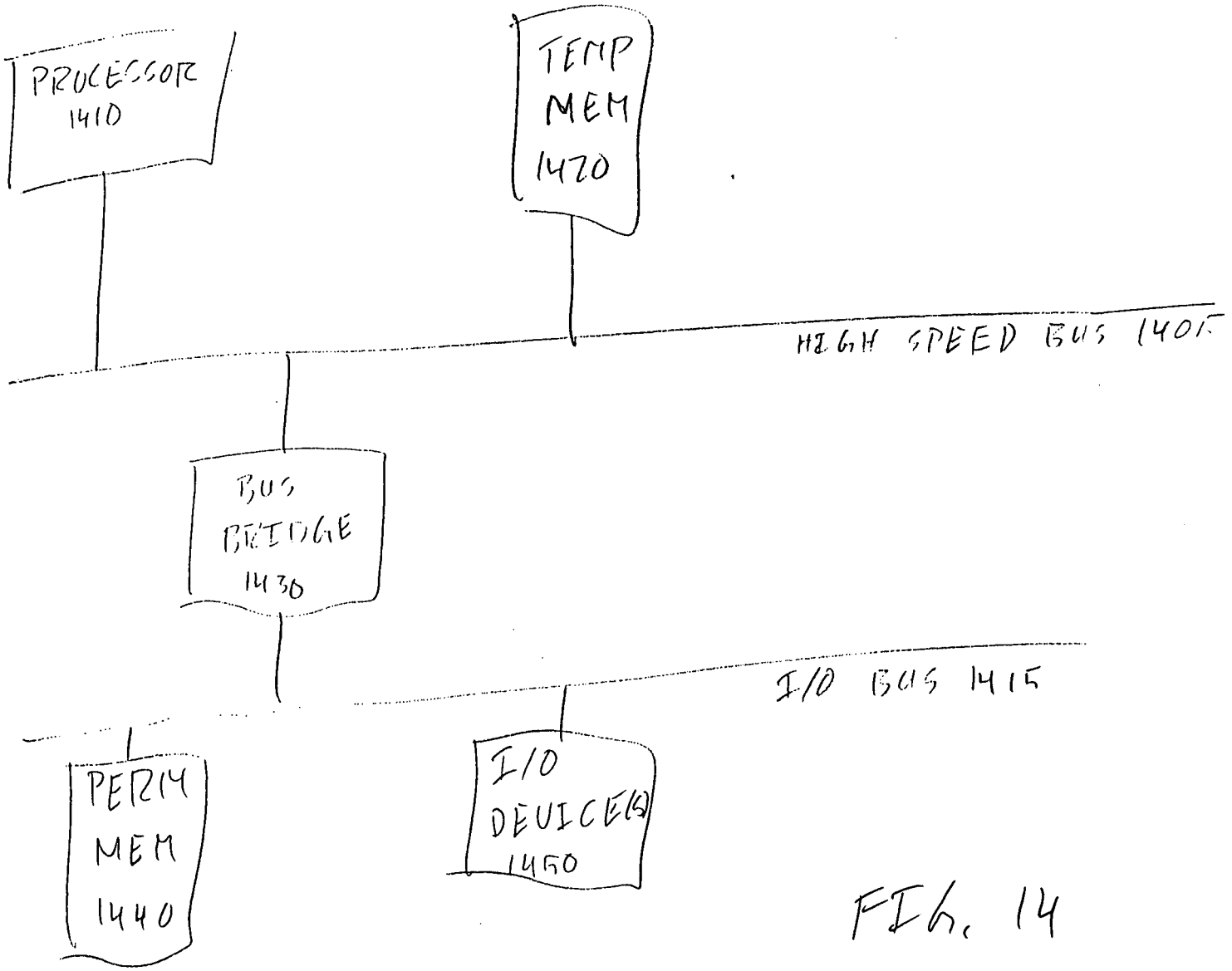


FIG. 14

0020h0" 562hh560

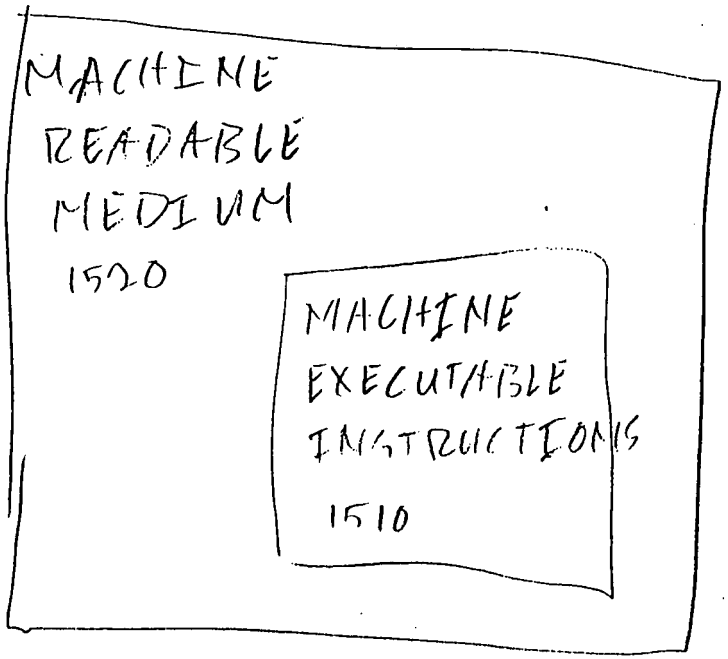


FIG. 15